

What is Claimed Is:

1 1. A secure detection network system having a plurality of nodes, each node comprising a
2 processor and storage means, the system comprising:

3 A. a plurality of remote nodes, each remote node comprising a set of detector
4 interfaces configured to couple to a set of detectors disposed to detect the
5 presence of an illegal asset within a shipping container;

6 B. at least one server node configured to initialize and install each remote node in the
7 plurality of remote nodes, including delivering to each remote node an agent
8 module, said agent module for each remote node comprising a node specific
9 configuration file defining a set of nodes with which the remote node can
10 communicate and a different encryption means corresponding to each node in the
11 set of nodes; and

12 C. a communication path coupling the plurality of remote nodes and the at least one
13 server node.

1 2. The system of claim 1 wherein the at least one server node includes a strobing module
2 configured to selectively initiate coordinated strobing of the encryption means among the
3 plurality of remote nodes.

1 3. The system of claim 1 wherein at least some of the plurality of remote nodes includes a
2 wireless communication means, the communication path includes an air path.

1 4. The system of claim 1 wherein the at least one server node includes a wireless
2 communication means, the communication path includes an air path.

1 5. The system of claim 1 wherein the at least one server node includes an audit module
2 configured to selectively cause one or more of the remote nodes to terminate communication
3 with at least one node in its set of nodes in response to one or more termination events.

1 6. The system of claim 5, wherein the one or more termination events includes detecting
2 tampering with one or more remote nodes.

1 7. The system of claim 1, wherein the illegal assets includes one or more of chemical
2 weapons, biological weapons or nuclear weapons.

1 8. The system of claim 1, wherein the illegal assets includes one or more of chemical
2 agents, biological agents, radioactive materials, illegal drugs, or explosive materials or devices.

1 9. The system of claim 1, wherein one or more remote nodes from the plurality of remote
2 nodes is disposed within a tamper resistant housing coupled to a shipping container.

1 10. The system of claim 1, comprising one or more subnetworks comprising a set of remote
2 nodes from the plurality of remote nodes, and wherein each subnetwork provides a portion of the
3 communication path.

1 11. The system of claim 1, further comprising:

2 D. a robot node, having a robot agent module and an interface to the communication
3 path, the monitor node including means to query each of the plurality of remote
4 nodes.

1 12. The system of claim 11, wherein the robot node is configured to query one of the
2 plurality of remote nodes via a set of other remote nodes from the plurality of remote nodes.

1 13. The system of claim 1, further comprising:

2 D. a monitor node coupled to the communication path and configured to audit the
3 plurality of remote notes.

1 14. The system of claim 13, wherein the at least one monitor node and the at least one server
2 node are configured to communicate with at least one remote node from the plurality of remote

3 nodes via one or more other intermediate remote nodes.

1 15. The system of claim 1, further comprising an orthogonal means of authentication.

1 16. A system of claim 1, wherein at least one remote node is housed within a tamper resistant
2 package with at least one detector.

1 17. A secure detection node comprising:

2 A. a secure network interface, configured to receive an agent module and
3 configuration files via a secure network;

4 B. a processor and a memory, the processor configured to execute the agent module,
5 the agent module configured to implement the configuration files to establish a
6 different encryption means for each node from a set of nodes with which the
7 secure detection node is to communicate; and

8 C. a detector interface, configured to receive data from a set of detectors disposed to
9 detect the presence of an illegal condition.

1 18. The node of claim 17, further comprising:

2 D. a tamper resistant box within which the processor and memory are housed.

1 19. The node of claim 17, further comprising:

2 D. at least one detector from the set of detectors.

1 20. The node of claim 19, further comprising:

2 D. a tamper resistant box within which the processor, memory and at least one detector are
3 housed.

1 21. A method of providing a secure detection network system having a plurality of nodes,
2 each node comprising a processor and storage means, the method comprising:

3 A. providing a plurality of remote nodes, each remote node comprising a set of

4 detector interfaces configured for coupling to a set of detectors disposed for
5 detecting the presence of an illegal condition within a shipping container;
6 D. generating by at least one server node an intelligent agent module and a set of
7 node specific configuration files for each remote node in the plurality of remote
8 nodes, including defining for each remote node a set of other nodes with which
9 the remote node can communicate, including providing a different encryption
10 means corresponding to each node in the set other nodes;
11 E. downloading to each remote node via a communication path a corresponding
12 intelligent agent module and a corresponding set of node specific configuration
13 files; and
14 F. installing each remote node in the plurality of remote nodes, including executing
15 the corresponding intelligent agent module with the corresponding node specific
16 configuration files.

1 22. The method of claim 21 including strobing the encryption means among the plurality of
2 remote nodes.

1 23. The method of claim 21 further including providing for at least some of the plurality of
2 remote nodes a wireless communication means, the communication path including an air path.

1 24. The method of claim 21 further including providing a wireless communication means for
2 at least one monitor node, the communication path including an air path.

1 25. The method of claim 21 including selectively causing one or more of the plurality of
2 remote nodes to terminate communication with at least one node in response to one or more
3 termination events.

1 26. The method of claim 25, wherein the one or more termination events includes detecting
2 tampering with one or more remote nodes.

1 27. The method of claim 21, wherein the illegal condition includes the presence of one or
2 more suspicious materials, including chemical weapons, biological weapons, nuclear weapons,
3 chemical agents, biological agents, radioactive materials, illegal drugs, explosive materials or
4 devices, or shielding means.

1 28. The method of claim 21, wherein the illegal condition includes a suspicious activity,
2 including an attempt to defeat a remote node or detector.

1 29. The method of claim 21, including installing one or more remote nodes from the plurality
2 of remote nodes within a tamper resistant housing coupled to a shipping container.

1 30. The method of claim 21, including forming one or more subnetworks comprising a set of
2 remote nodes from the plurality of remote nodes, and wherein each subnetwork provides a
3 portion of the communication path.

1 31. The method of claim 21, further comprising:

2 E. monitoring the plurality of remote nodes with at least one monitor node, including
3 querying each of the plurality of remote nodes via the communication path.

1 32. The method of claim 31, wherein the at least one monitor nodes is a portable robot node.

1 33. The method of claim 31, including communicating between at least one remote node
2 from the plurality of remote nodes and the at least one monitor node or the at least one server
3 node via one or more other intermediate remote nodes.

1 34. A secure identification control system comprising:

2 A. at least one body sensor configured to sense biometric information from a body;

3 B. a handheld node comprising an interface to the at least one body sensor and an
4 interface to a secure network, wherein the handheld node is configured to record
5 biometric information, including information indicating removal of the body

6 sensor from the body;

7 C. the secure network including at least one server node configured to deliver to the

8 handheld node an agent module, said agent module comprising a node specific

9 configuration file defining a set of nodes with which the handheld node can

10 communicate and a different encryption means corresponding to each node in the

11 set of nodes;

12 D. a set of detectors configured to sense a handheld node location; and

13 E. an identification controller coupled to the secure network and configured to

14 generate an identification indication as a function of the handheld node location

15 and an authentication of the body from the handheld node, wherein such

16 authentication is a function of an indication from the handheld device that the at

17 least one body sensor had not been removed from the body.

1 35. The secure identification control system of claim 34, wherein the set of detectors includes

2 one or more detectors configured for communicating via florescent lights or by retroreflective

3 illumination.

1 36. The secure identification control system of claim 34, wherein the body is a passenger in a

2 vehicle.

1 37. The secure identification control system of claim 34, wherein the identification controller

2 is configured for granting access to a secure facility or area.

1 38. The secure identification control system of claim 34, wherein the identification controller

2 is configured for providing the identification indication to a friendly fire prevention detection

3 system.

1 39. An orthogonal authentication system, comprising:

2 A. a computer system having a user interface and access to a network;

3 B. a user authentication subsystem comprising user specific authentication data for a

4 plurality of users, and configured to authenticate a user as a function of
5 authentication information input at the computer system;

6 C. a biometric database, comprising user specific biometric data for a plurality of
7 users;

8 D. a facility access control system having access to the network and the biometric
9 database, and including at least one biometric sensor and an access controller
10 configured to grant access to a facility as a function of biometric data received
11 from the at least one biometric sensor corresponding to a set of user specific
12 biometric data in the biometric database; and

13 E. a computer network access controller configured to grant the user access to the
14 network as a function of an authentication of the user by the user authentication
15 subsystem and an identification of the user from the facility access control
16 system.

1 40. The orthogonal authentication system of claim 39, wherein the at least one biometric
2 sensor includes a face scanner, palm scanner, retina scanner or fingerprint scanner.

1 41. A method of providing orthogonal authentication for access to a computer network, the
2 method comprising the steps:

3 A. granting access to a facility having a computer system therein as a function of
4 sensing biometric data of a user that corresponds with stored user specific
5 biometric data;

6 B. entering user authentication data at the computer subsystem;

7 C. authenticating the user by one or more of:

8 1. comparing the entered user authentication data with stored user specific
9 authentication data; or

10 2. confirming the identity of the user employee by visual inspection;

11 D. granting the user access to the computer network if the user was granted access to
12 the facility in step A and authenticated in step C, else refusing access to the
13 network by the user.